



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,602	07/30/2001	Christopher P. Jalbert	04860P2441	5216

7590 12/14/2007
James C. Sheller
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2137

MAIL DATE	DELIVERY MODE
-----------	---------------

12/14/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/918,602

Applicant(s)

JALBERT ET AL.

Examiner

Michael Pyzocha

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 October 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-5,8-26 and 29-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-5,8-26 and 29-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Art Unit: 2137

DETAILED ACTION

1. Claims 1, 3-5, 8-26, and 29-41 are pending.
2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/30/2007 has been entered.

Specification/Claim Rejections - 35 USC § 112

3. The objection to the specification and rejection under the first paragraph of 35 U.S.C. 112 has been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

Art Unit: 2137

Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 3-5, 8-22, 24-26, and 29-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang, U.S. Patent No. 5,953,424, in view of Menezes (Menezes, Alfred J. Handbook of Applied Cryptography. CRC Press. 1997. pages 234-237) in view of (Simple Network Authenticating Key Exchange) (hereinafter Snake) and further in view of Matyas, Jr. et al. (US 6307938) (hereinafter Matyas).

As per claims 1, 20, 21, 22, 24, and 38-40, Vogelesang discloses a cryptographic method comprising: generating, at a first entity, a first public key M_B , the first public key M_B being session specific (Vogelesang: Col 16, lines 33-35); receiving, at a first entity, a second public key M_A , the second public key M_A being session specific (Vogelesang: Col 16, lines 36-38); generating, at the first entity, a first session key K_B and a first secret S_B , the first session key K_B being different from the first secret S_B , both the first session key K_B and the first secret S_B being computed from the second public key M_A (Vogelesang: Col 16, lines 39-67); encrypting, at the first entity, a first random nonce N_B with the first session key K_B or the first secret S_B to obtain a first encrypted result, the first random nonce N_B being unrelated to both K_B and S_B . (Vogelesang:

Art Unit: 2137

Col 16, lines 43-67); transmitting the encrypted random nonce from the first entity to the second entity (Vogelesang: Col 16, lines 64-67); receiving a response to the encrypted random nonce (Vogelesang: Col 17, lines 19-24); authenticating through determining whether the response includes a correct modification of the first random nonce N_B (Vogelesang: Col 17, lines 28-30).

Vogelesang teaches that a first random nonce may be encrypted at the first entity with a session key to obtain a first encrypted result (e.g. Col 16, lines 64-67). Vogelesang also teaches a number of secrets that are generated using the second public key (e.g. T , Y_D , and other values which qualify as a "secret" under MPEP 2111). However, Vogelesang does not appear to suggest that the first encrypted result may be double encrypted.

Menezes teaches that encipherment of a message more than once "may increase security" (Menezes: page 234). Further, illustrates the process whereby a message may be encrypted once with a first key and a second time with another key (Menezes: page 234, part (a)). Combining the ideas of Menezes with Vogelesang facilitates a system in which a message may be encrypted once with a first key (e.g. session key) (part d) and a second time with another key (e.g. secret). It would have been obvious to one of ordinary skill in the art at the time the

Art Unit: 2137

invention was filed to combine the ideas of Menezes with those of Vogelesang because doing so may increase security.

The modified Vogelesang and Menezes system fails to disclose the specific generation of the first secret.

However, Snake teaches generating a secret based on a function of a password, and two public values (see page 1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the secret generating method of Snake using the public keys of the modified Vogelesang and Menezes system as the public values.

Motivation to do so would have been to provide mutual authentication (see page 2).

The modified Vogelesang, Menezes, and Snake system fails to disclose creating a secret equal to a sequence of hash functions applied to the values.

However, Matyas teaches creating a secret equal to a sequence of hash functions applied to different values (see column 5 line 66 through column 6 line 12).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to apply the random number generation method of Matyas to the data of the modified Vogelesang, Menezes, and Snake system to obtain the secret value.

Art Unit: 2137

Motivation to do so would have been to obtain a value of a specific length longer than a single hash value would produce (see Matyas column 5 line 66 through column 6 line 12).

As per claims 3 and 4, the modified Vogelesang, Menezes, Snake, and Matyas system discloses checking whether a received modification of the first random nonce N_B equals a modification of the first random nonce N_B applied by the first entity (Vogelesang: Col 17, lines 25-37).

As per claim 5, the modified Vogelesang, Menezes, Snake, and Matyas system discloses generating a first random number R_B (Vogelesang: Col 16, lines 39-40); computing the first session key K_B from the second public key M_A raised to the exponential power of the first random number R_B , modulo a parameter B_B (Vogelesang: Col 16, lines 39-42).

As per claims 8-10 and 29-31, the modified Vogelesang, Menezes, Snake, and Matyas system discloses the combining function is a hash function (see Snake page 1).

As per claims 11 and 32, the modified Vogelesang, Menezes, Snake, and Matyas system discloses combining the values to arrive at a first and second result (see Snake page 1 message 3 and 4 where the key is calculated on each side)

As per claims 12 and 13, the modified Vogelesang, Menezes, Snake, and Matyas system discloses wherein the first random

Art Unit: 2137

nonce is encrypted using a symmetrical encryption algorithm (Vogelesang: Col 16, lines 64-67).

As per claims 17-19, the modified Vogelesang, Menezes, Snake, and Matyas system discloses extracting the second random nonce N_A from the response (Vogelesang: Col 16, line 39 to Col 17, line 28); modifying the second random nonce N_A to obtain a modified second random nonce (Vogelesang: Col 16, line 39 to Col 17, line 28); encrypting the modified second random nonce using the first session key K_B and the first secret S_B to obtain an encrypted package (Vogelesang: Col 16, line 39 to Col 17, line 28); transmitting the encrypted package from the first entity (Vogelesang: Col 16, line 39 to Col 17, line 28).

As per claim 26, the modified Vogelesang, Menezes, Snake, and Matyas system discloses generating a first random number R_B (Vogelesang: Col 16, lines 39-40); computing the first session key K_B from the second public key M_A raised to the exponential power of the first random number R_B , modulo a parameter B_B (Vogelesang: Col 16, lines 39-42).

As per claims 34-37, the modified Vogelesang, Menezes, Snake, and Matyas system discloses generating a first random number N_B (Vogelesang: Col 16, line 33 to Col 17, line 27); encrypting a combination of the first random number N_B and the

Art Unit: 2137

modified second random number (Vogeleang: Col 16, line 33 to Col 27, line 27).

As per claims 14-16, 25, and 33, the modified Vogeleang, Menezes, Snake, and Matyas system discloses wherein encrypting the first random nonce N_B includes superencrypting the first random nonce N_B (Menezes: pages 234-237).

As per claim 41, the modified Vogeleang, Menezes, Snake, and Matyas system discloses wherein the network is a network operating according to a hypertext transfer protocol and the first public key M_B is transmitted for session key exchange before the encrypted second random number is received (Vogeleang: Col 1, lines 12-14; Col 16, lines 25-67).

5. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Vogeleang, Menezes, Snake, and Matyas system.

As per claim 23, the modified Vogeleang, Menezes, Snake, and Matyas system discloses a network operating according to a hypertext transfer protocol and the first public key M_B is transmitted with the encrypted random nonce for session key exchange.

The modified Vogeleang, Menezes, Snake, and Matyas system does not disclose transmitting the first public key M_B with the encrypted random nonce. Applicant's failure to argue the

Art Unit: 2137

previous official notice of the subject matter of claim 23 is taken as acquiescence that the subject matter of claim 23 is obvious (See MPEP 2144.03). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to transmit a key with a nonce because doing so is more efficient than having to make two separation transmissions for the key and the nonce.

Response to Arguments

6. Applicant's arguments filed 10/30/2007 have been fully considered but they are not persuasive. Applicant argues that none of the cited references teach or suggest using a sequence of hash functions; and the references cannot be combined.

Applicant's argument that using a sequence of hash functions is moot based on the new grounds of rejection.

With respect to Applicant's argument that the references cannot be combined because Vogelesang encrypts private data while Snake encrypts public messages, the Examiner respectfully disagrees. Snake encrypts the values R and S which are random numbers on each the client and server side. These values are not known but the other until they are sent, received and decrypted by the other. Therefore, both Vogelesang and Snake teach methods of encrypting private data and can be combined.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER